April 2016

Volume 1, Issue 7

Security Matters

Focus on Passwords

In this increasingly digital world we live in, passwords are the keys to nearly everything we do. We use them to access email, social media, bank accounts, online shopping, health care records, our child's school website – not to mention all the systems we use at work each day. With just a password, a malicious person could empty your bank account, sabotage a system where you work, view your health care information, or even steal your identity. The tips and tricks here can help you create strong passwords and manage them safely.

State of Montana policy requires that you have a password that is at least eight characters long and must be changed every 60 days. In addition, your password should contain uppercase, lowercase, numeric, and special characters. The password "Hacked1!" is an example of a password which meets all the suggested criteria but still is a weak password that could be cracked in less than one day. Clearly, meeting the minimum requirements isn't good enough.

The first problem with Hacked1! is that it uses a dictionary word as its main component. Dictionary words in any language are very easy to crack, as are names of people and places. Adding a number and/or special character at the end of a word is common and easily cracked. Hacked1! is also only eight characters. By policy, that is the minimum required, but longer passwords are more secure passwords, so follow that rule whenever you can.

So how do we make stronger passwords while still making them memorable? One way is to use a phrase as the starting point for your password. For example, let's use the phrase "these are a few of my favorite things". Using the first letter of each word, it would be "taafomft". That's a weak password, but we can make it better by using uppercase in places and by substituting numbers or special characters: "t@Af0mf7". To make it truly strong, we should add to the length, perhaps by defining some of our favorite things like kittens, puppies, and babies, resulting in "t@Af0mf7:KP&b". The addition of those five characters on the end takes this password from

Continued on page 5

Along with the National Cybersecurity Alliance (NCSA) and the Better Business Bureau (BBB), the Enterprise Security Program (ESP) is encouraging everyone to add their digital devices to their spring cleaning lists in April.

This new spin on spring cleaning can help you be more secure online, protect valuable personal information, and avoid identity theft.

To get started, download NCSA's **Digital Spring Cleaning Checklist** and create an action plan that assigns tasks to the appropriate person.

The easy-to-follow timeline and plans breaks it down into weekly goals:

Week 1: Keep Clean Machines.

- Keep all critical software current.
- Clean up your mobile life by reviewing app permissions and deleting or uninstalling unused apps and software.

Continued on page 2

SITSD
Enterprise Security
Program

Security Matters is the monthly information security newsletter published by the Enterprise Security Program. Each month we also have a supplemental file of materials you can use for security awareness. You can find that file at: http://sitsd.mt.gov/Montana-Information-Security/Security-Training-Resources

We hope you'll find the newsletter and materials useful and hope you'll give us feedback on what we can do better. Your suggestions for topics and content are welcome. Contact us.

Inside this issue:

A monthly update on the latest security threats and other software news.

Sean Rivera, CISSP

DROWN Vulnerability – The latest vulnerability to have a major worldwide impact is called DROWN, which stands for Decrypting RSA with Obsolete and Weakened Encryption. Researchers published the vulnerability at the end of February. At that time, nearly one third of HTTPS websites in the world were vulnerable to this configuration issue.

The use of SSL version 2 was discouraged almost 20 years ago as a result of vulnerabilities and a more secure protocol being created. If a website still permitted SSL version 2 connections an attacker could leverage that vulnerable connection to intercept the more commonly used TLS protocol on HTTPS sites and perform a man-in-the-middle attack. An attacker could also compromise a websites TLS certificate if it was shared with other servers where any one server had the SSL version 2 connection enabled.

SITSD has worked diligently to communicate with all agencies that were vulnerable and taken appropriate steps to remediate. If system administrators have any questions, they should visit https://drownattack.com, contact the SITSD Service Desk at 444-2000, or send an email to servicedesk@mt.gov.

Tax Fraud Phishing – The month of February was particularly busy for multiple private-sector businesses reporting data compromises involving employee tax information. In what are being labeled Business Email Compromise attacks, attackers are leveraging the inherent trust employees have with their leadership and requesting data that would allow an attacker to perform tax fraud. Companies such as SnapChat, Seagate, and Polycom, just to name a few, reported that they fell victim to such attacks, willfully providing payroll information to attackers who spoofed emails from executive-level leaders. Security experts all state that if a system of checks and balances had been enabled in which employees would be allowed to verify such requests without any negative effects from the established leadership that none of these attacks would have been successful.

Employees who receive requests that may seem unusual or potentially suspicious should contact their immediate supervisors to request assistance.

Security Awareness 2016 Events

Focus on Passwords

- April 14, 2016 - 1:30—3:30 at the OPI Training Room
  1227 11th Ave

♦♦♦♦♦♦♦♦♦♦♦♦♦♦

Check Montana Information Security for the latest event schedule and contact Lisa Vasa if you'd like to host an event.

Spring continued from page 1

Week 2: Make Sure You're Secure

- Turn on two-step authentication when available. Not sure about availability? Visit: https://twofactorauth.org/
- Make sure your router has a strong password and check for updates to the router's software.
- Change your account passwords for your accounts after reading the advice in this newsletter.
- Secure your phone with a passcode, passphrase, or finger print.

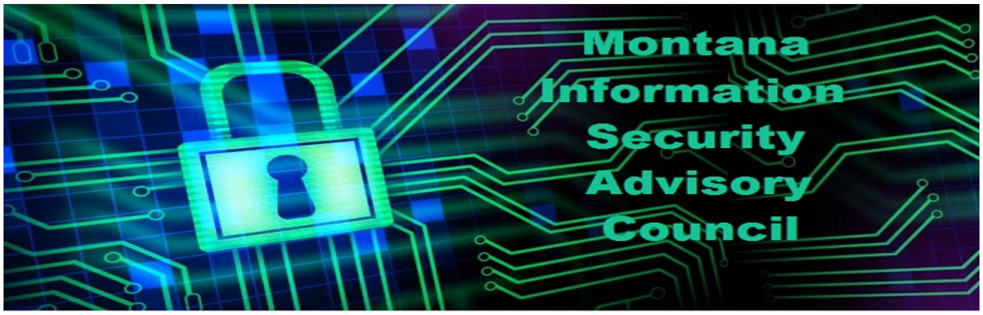
Week 3: Digital File Purge and Protection

- Clean up your email and keep only those you really need.
- Review your digital subscriptions and unsubscribe to those you no longer read.
- Dispose of electronics securely. Don't just throw electronics in your trash. **The State of Montana Quarterly Recycling Drive** is April 8, 2016 in the South Lockey parking lot behind the Capitol. Please contact Matt Elsaesser at Helena Industries for more information. He can be reached at 442-8632 or melsaesser@helenaindustries.org.
- Update and backup your online photo album.
- Review friends on social networks and contacts on your phones to make sure everyone on those lists still belongs.
- Backup up important files to another drive or to the cloud. Commit to doing backups regularly.
- Don't forget to empty your trash or recycle bin to permanently delete old files.

Week 4: Clean Up Your Online Reputation

- Review the privacy and security settings on websites you use to be sure the settings are acceptable to you.
- Clean up your social media presence by deleting old photos or posts that are embarrassing or no longer represent who you are.
- Review your personal information on social media sites and update if needed.

Meeting Highlights of the Montana Information Security Advisory Council Meeting & Preview of the Upcoming Meeting



March 17, 2016

Meeting highlights

University security incidents

Adrian Irish provided an overview of two recent information security incidents. First, the University of Montana experienced phishing attempts during January and February of 2016. The perpetrators were attempting a wire transfer scam by imitating important members of the university system.

Secondly, on December 24, 2015, the University of Connecticut's (UConn) domain was hijacked. The attackers exploited a weakness in the .edu domain password reset system. When a password reset is requested, the domain sends a password reset token to everyone on the site administrator list. The attackers had compromised and gained access to the email of one of the fifteen administrators, and were able to trigger a password reset. Irish noted that in situations like this, multi-factor authentication would be beneficial.

Security Topic: MT-Drive and OneDrive for Business

Margaret Kauska discussed the state's use of OneDrive and MT-Drive, and asked for clarification regarding its security. MT-Drive and OneDrive for Business are secured Enterprise solutions.

OneDrive is for document storage internal to the state only.

MT-Drive is used for sharing files with users outside of the state's network. MT-Drive is a function within the file transfer service, and is secured by active directory for state employees. For public access, MT-Drive is secured by ePass Montana. For those users the system is secured by two-step verification: the user must have an established ePass account; and the request is verified via email. Both data in transit and data at rest are encrypted.

Transferring a file requires a state employee to either be sending or receiving. State employees can establish an MT-Drive folder and can then control permissions for public access. If a state employee leaves, the MT-Drive folder becomes accessible by his or her supervisor. Local governments that are on SummitNet can also take advantage of MT-Drive for free.

MT-Drive has a full audit records and can be tracked by agency. SITSD maintains full audit records for file permissions and all upload and download events. Files received via MT-Drive undergo a full virus scan.

OneDrive for Business is stored in the Microsoft cloud, and is part of the Sync tool within Office. Files are saved locally and then synced to the cloud. Everything is encrypted at all times. Use of OneDrive is restricted to state employees. When an employee leaves, his or her supervisor is notified and must choose what to do with the leftover data.

Data loss protection (DLP) and rights management are prerequisites for access to OneDrive outside the state network. Microsoft is currently working on implementing DLP, and has given a tentative timeline of around six months.

Microsoft provides a web portal and users can log in with their state active directory credentials to access web-based Office apps and OneDrive files. They can be edited and saved back into OneDrive without leaving a copy on the home computer. This can also help prevent saving files to USB hard drives and taking those documents outside the office. There is also a mobile app where users can access OneDrive files from their smartphones.

MT-ISAC Workgroup Updates

Assessment Document

The Assessment Workgroup has developed an assessment document for agency security officers to use to track their agency's compliance with the Information Security Policy. The document is posted on the MT-ISAC website. This document is intended to be utilized by the agency and shared with the State CIO. It will not be public due to the sensitive nature of the document's content.

National Cyber Security Review (NCSR)

The Multi-State Information Sharing and Analysis Center (MS-ISAC) National Cyber Security Review (NCSR) was voted on and approved by the Council to be used for agencies yearly reporting to the Governor. This online questionnaire will be released in the fall and will give agencies and the Governor a snapshot of their current security posture. Once the survey is completed and compiled by MS-ISAC, agencies will be able to compare their security posture with corresponding state agencies as well from other states. The survey should take several hours to complete if you know your environment well. The 2015's NCSR question set has been posted to the MT-ISAC website for those who would like to review.

Small Incident Handling

The Best Practices workgroup recently completed a Small Incident Handling document and it is currently being reviewed by the Council. A vote on approval will be an action item in April. The Small Incident Handling document includes step-by-step instructions including a flowchart for handling incidents such as malware infections. This has also been posted to the MT-ISAC website.

Information Security Incident Report Form

The Council approved the Information Security Incident Report Form that was submitted by the Situational Awareness workgroup. This form is to be filled out if there is an incident of high or critical nature. The form can be found on the Mine page, under IT Professional Information tab within the Security section. https://mine.mt.gov/it/pro/default.mcpx

Next Meeting

The next meeting will be **Thursday,** April 21, 2016 at 1:00 p.m. at the Capitol, Room 350.

For more information and posted documents, please visit:

MT-ISAC website

Security Training News

SANS Securing the Human Training Reminder

April 1st marks the half-way point for the SANS Securing the Human training year. All executive branch employees are required to take this training annually, so if your agency hasn't yet started training, consider rolling it out soon to give staff time to finish their training.

Also, June 15, 2016 is the deadline for having training completed in order to qualify for the General Liability Insurance discount with the DOA Risk Management and Tort Division (RMTD).

Using the Hold subaccount. It's a great idea to keep your SANS account updated throughout the year as employees come or go. We especially encourage you to use your Hold account for terminated users so we know to remove them at the end of the training year. If they aren't removed during the year-end reset, they will hold a training license unnecessarily—a license that could be used for a current user.

We'd also like you to take a look at any inactive users and either remove them or move them to the Hold account so we can remove them now. We are getting short on licenses and if we can free up some additional seats we may be able to avoid purchasing more. Contact Lisa Vasa with any questions.

Congratulations to Jeannene Maas of the Department of Commerce for winning the Microsoft Surface Pro 4! Jeannene attended the Security Awareness event at the Park Avenue Building in February.

We will be giving away another Surface in September. Attend a Security Awareness event for your chance to win.

Information Assurance Compliance

Fed VTE Live! Program—May 10 or May 12, 2016 at 7:00 am to 3:00 pm MDT **Two sessions will be held.**

The course begins with a survey of laws, regulations, and standards that drive IA Compliance practices, and then quickly shifts into a practical coverage of how that knowledge is implemented through the Risk Management Framework (RMF) to secure enterprise IT systems. All training is built to support student engagement in a federal Business Case Analysis that will teach students how to categorize a system as low, medium, or high risk, how to select appropriate security controls to mitigate risk, and how to develop an action plan that leads to a successful Security Authorization Decision. Topics and hands-on activities will engage the student to learn IA practices that ensure appropriate treatment of risk, compliance, and assurance from internal and external perspectives. Applications must be received prior to April 28. For more information, contact Lisa Vasa.

Open Season on Cyberthreats: Threat Hunting 101 (Part 1) & Threat Hunting Methodologies and Tools (Part2)

Virtual Event—April 14, 2016 11:00 AM MDT & April 15, 2016 11:00 AM MDT

In Part 1 of the webcast, attendees will gain insight into what threat hunting entails; what pitfalls stand in the way of attaining actionable results; and what organizations are discovering through threat hunting. In Part 2 attendees will learn about what tools organization are using for threat hunting; what skills hunters need; and how threat hunting affects and is affected b y security budgets. More information and registration.

Virtual Training Environment (FedVTE)

We want to remind you about the FedVTE cybersecurity training system. Courses range from beginner to advanced levels and are available at no cost to users. Sign up is easy at: www.Fedvte.usalearning.gov and a catalog of available courses is on the site. Also, look for announcements regularly for opportunities to participate in the FedVTE Live! Classes. These classes use an interactive virtual live classroom and are the next best thing to being there. Space is limited so respond quickly to announcements if you are interested.

For more security training and awareness resources, check out the Security Training Resources page and watch for more information here each month.

Focus continued from page 1

something that could be cracked in a day to one that would take 423 centuries to crack!

Another quick tip for remembering a complex password is to use the “three and random” rule: pick three words that have meaning to you, but would seem random to someone else. For example, you might choose green, Norwegian, and bicycle because green is your favorite color, your grandfather was Norwegian, and you love to ride your bicycle. Combine them and change them up like we did with the passphrase and you’re good to go!

Remember these tips for creating passwords:

- **Do make your password more than eight characters if possible. Longer is better.**
- **Do make them something you can easily remember, but others wouldn’t guess.**
- **Do use a mix of uppercase, lowercase, numbers, and special characters.**
- **Don’t use single dictionary words, names, or places as your password.**
- **Don’t just substitute numbers or special characters for lookalike letters in a word.**
- **Visit http://passfault.com/ and test your password.**

Stop and think for a minute. How many systems or sites do you use that require a password? For every different site, account, or system you should have a different password. It’s not uncommon for people to use the same password for most, if not all, of their accounts. The danger to this is when one site is compromised and your credentials stolen, the bad guys have access not just to your Facebook account, but your bank account or work systems as well. Here are some suggestions for dealing with all those passwords you need to remember.

Use a similar password, but with identifiers to tell you what site or system for which the password is used. First create a strong static password using what you learned above. Then make up a set of rules that help you identify where the password will be used. For example, use the first letter of the name or the application or site, the last letter of the name of the site, and the number of letters in the name. For example, using the “t@Af0mf7” password, the password for your Amazon account would be “aN6t@Af0mf7”. This also addresses the issue of adding length to a password based on a short phrase. Use rules that make sense for you and don’t share them with others.

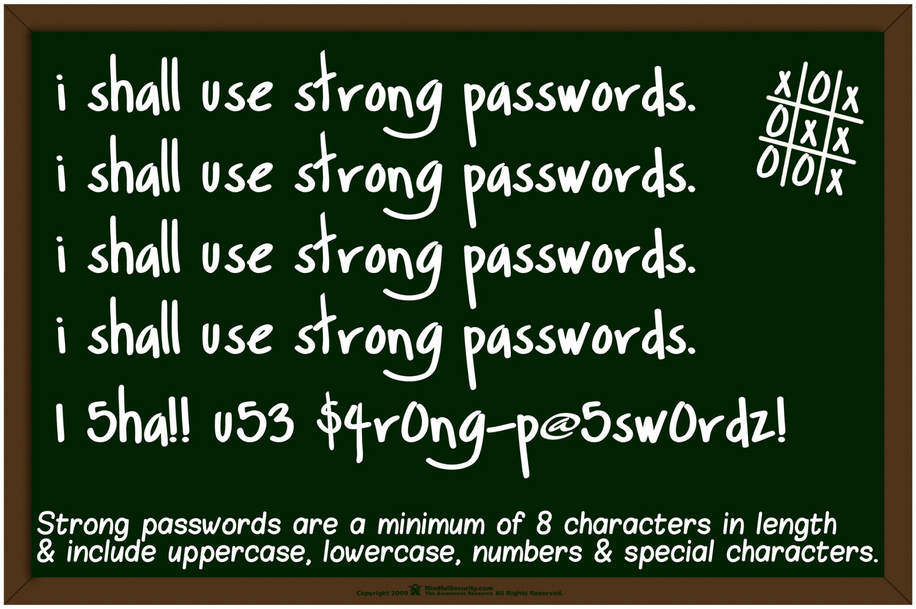
Another way to keep multiple passwords secure is to use a password manager. Password managers, safes, or vaults are digital tools for storing password and account information. They may be on your local device or you may use a server-based or cloud-based manager. With a password manager, you need only remember one password – the one you’ll use for the manager itself. Some password managers take the matter of secure passwords one step further and generate strong passwords for you.

Three things to remember if you choose to use a password manager: 1) make sure the master password is something you will remember. Losing it means losing everything in your password manager; 2) make sure to backup your password manager; and 3) if you are planning to use a password manager at work, make sure it has been approved by your management.

A few last tips about passwords:

- **Change your passwords regularly. Yes, even your non-work related passwords.**
- **Never share your password with others. If someone has a legitimate need to have you logged on to a system (perhaps for tech support), always enter your credentials yourself rather than telling them your password.**
- **Never write down your passwords and leave them under your keyboard, on a sticky note on your computer, in an unlocked desk drawer, or other place where they could be found by someone.**
- **Don’t forget to use strong passwords on your mobile devices, too.**
- **When available, use two-factor authentication to provide additional protection.**

By making your password strong and secure, you protect your information, your identity, and your workplace.


i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
i shall use strong passwords.
I 5ha!! u53 $4r0ng-p@5sw0rdz!
X O X
O X X
O O X
Strong passwords are a minimum of 8 characters in length
& include uppercase, lowercase, numbers & special characters.

News You Can Use

1 in 5 Employees Are Willing To Hand Over Their Work Passwords For Money

A new survey from SailPoint—a firm that sells software for managing user access—found the 20% of respondents (all from companies with at least 1000 employees) would sell their work passwords to a third part for a fee.

25 Worst Passwords of 2015

Every year SplashData compiles a list of stolen passwords then sorts them in order of popularity. Trust us, you don't want your password to be on this list!

5 Things You Need To Know About Two-Factor Authentication

Having a strong password is important, but enabling two-factor authentication provides more protection than even the strongest password.

WE KNOW YOU LOVE SECURITY CAT
Password: Tiger
BUT DON'T BLOW HIS COVER AND USE HIS REAL NAME AS YOUR PASSWORD!
NEVER USE YOUR PET'S NAME AS YOUR PASSWORD! THAT'S TOO EASY FOR CRIMINALS TO GUESS
YOUR PASSWORD SHOULD BE HARD TO GUESS BUT EASY TO REMEMBER
SAC the security awareness COMPANY
© 2014 THE SECURITY AWARENESS COMPANY

Security Quick Tip

Password managers can be a huge help in keeping track of all your passwords, but if you're using one, make sure that the master password itself is long, strong, and memorable only to you.

For more security tips, news, advisories, and resources visit the Montana Information Security website, find us on Facebook, or follow us on Twitter.

http://sitsd.mt.gov/MontanaInformationSecurity

State of Montana Information Security

@MontanaSecurity

Contact Us:

Enterprise Security Program

Lynne Pizzini, CISO and Deputy Chief Information Officer

Joe Frohlich, Enterprise Security Manager